BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

98 P 2643

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 28 045 A1**

B1

(51) Int. Cl.[6]:
G 06 F 17/60
G 06 F 12/14
G 07 F 19/00

(21) Aktenzeichen: 196 28 045.1
(22) Anmeldetag: 11. 7. 96
(43) Offenlegungstag: 22. 1. 98

(71) Anmelder:
ESD Information Technology Entwicklungs GmbH, 04430 Dölzig, DE

(74) Vertreter:
Haußingen, P., Ing. Faching. f. Schutzrechtswesen, Pat.-Anw., 06526 Sangerhausen

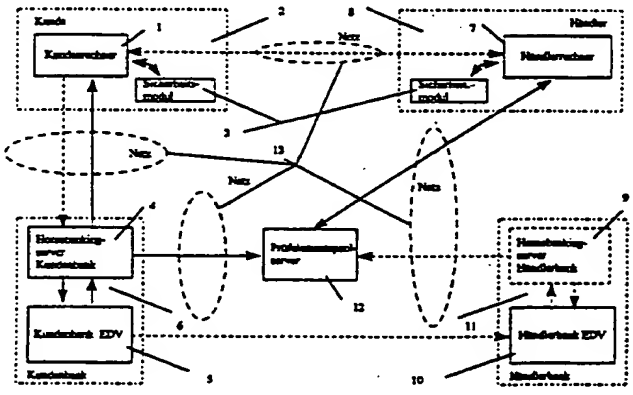
(72) Erfinder:
Antrag auf Nichtnennung

(56) Entgegenhaltungen:
DE 43 33 388 A1
US 54 65 206

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Anordnung zur Integration von Kunden/Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze

(57) Die Erfindung betrifft ein Verfahren und eine Anordnung zur Integration von Kunden/Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze.
Aufgabe der Erfindung ist es, ein preiswertes und unkompliziertes Verfahren zur Abwicklung von Zahlungen auf digitalen Netzen durch Einbeziehung von vorhandenen Zahlungsstrukturen zu entwickeln.
Nach Figur (1) wird die Aufgabe dadurch gelöst, daß mit einem Sicherheitsmodul (3), aus einem Homebankingserver Kundenbank (4), einer Kundenbank EDV (5) der Kundenbank (6), dem Händlerrechner (7) des Händlers (8) mit dem Sicherheitsmodul (3), optional aus einem Homebankingserver Händlerbank (9), der Händlerbank EDV (10) der Händlerbank und einem Prüfelementepoolserver (12), wobei dieser von dem Händlerrechner (7), der Kundenbank EDV (5) und der Händlerbank EDV (10) über ein Netz (13) erreichbar ist und die Zahlungsanweisungen von dem Händlerrechner (7) über den Kundenrechner (1) an den Homebankingserver Kundenbank (4) in die Kundenbank EDV (5) zur Händlerbank EDV (10) g leitet w rden, wobei der Händler (8) die Gültigkeit der Zahlungsanweisung mit Hilfe von Daten aus dem Prüfelem ntepoolserver (12) selber prüfen und ohne Verzögerung die Waren Dienstleistung n (33) an den Kunden (2) ausliefern kann.



DE 196 28 045 A1

DE 196 28 045 A1

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen durch Anbindung an vorhandene Zahlungsstrukturen. Die Erfindung ist einsetzbar zur Abwicklung von Geschäften über digitale Netzwerke wie dem Internet und anderen Netzwerken.

Immer häufiger werden Geschäfte über digitale Netzwerke, wie dem Internet oder andere Netze, abgewickelt. Dabei spielt die Art der Zahlung und die Zahlungsabwicklung eine wichtige Rolle. Waren oder Dienstleistungen können sehr einfach angeboten werden, aber die Abwicklung der Zahlung stellt ein großes Problem dar. Bisher wurden verschieden Ansätze zur Lösung des Problems gefunden, wobei jede der Lösungen, sowohl aus einer technischen Komponente, z. B. aus einer Verschlüsselungssoft- oder Hardware, als auch aus einer Prozeßkomponente besteht.

Eines der bekannten Verfahren zur Abwicklung von Zahlungen wird z. B. von VISA und MASTERCARD propagiert. Dabei handelt es sich um das SET-Protokoll mit dessen Hilfe Kreditkartendaten verschlüsselt und die verschlüsselten Kreditkartendaten vom Kunden an den Händler übertragen werden. Der Händler überträgt anschließend seinerseits diese Daten an die nächste Clearingstelle, wo das eigentliche bekannte Kreditkartenclearing ausgeführt wird. Die Kosten für das Verfahren sind also mit den Kosten der Kreditkartenorganisationen belastet. Zusätzlich ist zu beachten, daß in vielen Ländern keine Kreditkarten (oder die Kreditkarten nicht in dem Maße) genutzt werden. Folglich können die Nutzer von Kreditkarten in solchen Ländern nicht mit diesen Kreditkarten bezahlen.

Des weiteren sind die Kosten für die Händler, die eine Kreditkartenzahlung akzeptieren, relativ hoch, was den Gewinn an den verkauften Gütern oder Dienstleistungen verringert. Es ist weiterhin anzumerken, daß das Risiko für einen Zahlungsausfall bei der Kreditkartenorganisation gegenüber dem Kunden relativ hoch ist und der Kunde gegenüber dem Händler nicht anonym bleibt.

Ein weiteres Verfahren ist das Bezahlen über digitales Geld, ob in Form einer Chipkarte oder in Form von ladbaren Ziffernfolgen, wie es bei DIGICASH möglich ist. Die Verfahren benötigen jedoch eine aufwendige Abwicklung. Es muß eine emittierende Stelle gefunden werden, bei welcher der Kunde sein "echtes Geld" hinterlegt oder per Kreditkarte "virtuelles Geld" kauft. Die Emission und die Prozeßkosten für ein solches virtuelles Geld sind aus nachfolgend aufgeführten Gründen relativ hoch:

1. Der Kunde muß sich bei der Bank melden, identifizieren und einen Geldbetrag anfordern. Dazu muß die Bank aufwendige Rechenschritte vollziehen, in denen verschiedene kryptologische Prozesse ablaufen, die relativ viel Rechenleistung benötigen.
2. Der Kunde kann nun mit dem von Ihm erhaltenen digitalen Geld bei einem Händler bezahlen, der diese Art der Zahlung akzeptiert, indem er eine bestimmte Menge dieser digital signierten Zahlen an den Händler überträgt.
3. Der Händler muß sofort Kontakt mit der Bank aufnehmen und überprüfen, ob er wirklich gültiges digitales Geld erhalten hat und nicht jemand unberechtigt versucht, mit gefälschtem digitalen Geld zu bezahlen.
4. Die Bank überprüft, ob schon einmal mit diesem digitalen Geld bezahlt wurde. Ist dies nicht der Fall, streicht sie das Geld aus der Liste der digital ausgegeben Geldbeträge heraus und meldet dem Händler, daß er sein Geld demnächst bekommen wird.
5. Der Händler meldet dem Kunden zurück: "Alles ist in Ordnung, die Ware kann geliefert werden."
6. Es muß darauf geachtet werden, daß das digitale Geld auch relativ schnell altert. Da es über ein digitales Signaturverfahren mit Hilfe asymmetrischer Algorithmen, wie RSA, geschützt wird, werden bestimmte Private Key und Public Key verwandt, die in endlicher Rechenzeit berechnet werden können. Deshalb muß das Geld immer wieder aufgefrischt werden, bevor ein theoretisches Nachrechnen der Private Keys möglich ist. Dies erzeugt relativ hohe Kosten im Prozeßablauf und in der Verwaltung, so daß diese Kosten ebenfalls von den Kunden oder von den Händlern gedeckt werden müssen. Gleichzeitig stellt sich als Problem dar, daß die Einnahmen aus DIGICASH und Kreditkartengeschäften in die bestehende Buchführung des Händlerunternehmens eingegeben werden müssen. Damit kommen zusätzliche Kosten auf den Händler zu, da er eine neue Zahlungsform in seine Buchhaltung integrieren muß, was bei großen Unternehmen zu erheblichen Summen führt.
7. Digitales Geld bringt ebenfalls das Problem der Geldmengenkontrolle mit sich. Hier wird eine neue Zahlungsform, eine Art neues Geld eingeführt, was nur schwer kontrolliert werden kann.

Alle anderen Verfahren sind zumeist mit einem der beiden Systeme DEBIT oder dem Kreditkartensystem verwandt und werden in ähnlicher Form abgewickelt.

Neben den sehr hohen Prozeßkosten, kommt noch eine sehr starke Sicherheitsproblematik hinzu. Digitales Geld kann natürlich sehr einfach von der Festplatte des Besitzers kopiert werden. Bei der Kreditkarten- oder bei der Chipkartenlösung ist das Problem ebenfalls nicht zur Genüge gelöst, weil die Rechner der Endkunden, von denen die Zahlungsinformationen an den Händler oder an die Bank übertragen werden, unsicher sind. Durch den Anschluß an das Internet, ist die Sicherheitsstufe des Rechners identisch mit der Sicherheitsstufe des gesamten Netzes. Damit kann auf dem Rechner des Kunden relativ einfach über einen Trojaner oder über einen Computervirus zugegriffen werden. Dieser Virus könnte bspw. die. Datei mit dem DIGICASH kopieren und auf eine bestimmte Adresse versenden oder eine Überweisung vom Rechner des Kunden ausführen.

Zusammenfassend ist keine der bisher bekannten Lösungen im Ablauf hinreichend unkompliziert und bezüglich der Sicherheit des Systems genügend auf digitale Angriffe vorbereitet.

Aufgabe der Erfindung ist es, ein preiswertes und unkompliziertes Verfahren zur Abwicklung von Zahlungen auf digitalen Netzen durch Einbeziehung von vorhandenen Zahlungsstrukturen zu entwickeln, wonach die Kunden und die Händler preiswert Zahlungen vornehmen und dabei auf bestehende Infrastrukturen zurückgreifen können sollen und die Sicherheit gegenüber digitalen Angriffen gewährleistet werden soll.

Erfindungsgemäß wird die Aufgabe durch die im Patentanspruch 1 aufgeführten Merkmale gelöst.

Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Die Vorteile der Erfindung bestehen darin, daß die Zahlungsproblematik in digitalen Netzen gelöst werden kann, ohne eine neue Geldart oder Währungsart einzuführen, jedoch mit wesentlich geringeren Abwicklungskosten als die bisher bekannten Zahlungsverfahren. Dabei wird auf bestehende Infrastrukturen zugegriffen, die bisher nicht geeignet waren, digitale Zahlungsströme anzunehmen oder digitale Zahlungen abzuwickeln. Die Lösung erzeugt keinen großen Datenverkehr auf den digitalen Netzen und es bedarf keiner Bestätigungen bei dritten Instanzen für die Echtheit der Zahlung. Die Anonymität der Zahlungen kann optional gewährleistet werden. Die Prozeßsicherheit des Systems wird gegenüber bisherigen Debitor-, Kreditorsystemen wesentlich erhöht und für den Kunden flexibler gestaltet. Jeder Kunde kann sehr einfach ebenfalls zum Händler werden, ohne das er andere technische Voraussetzungen schaffen muß.

Die Erfindung wird mit

Fig. 1 als Integrationssystem zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen,

Fig. 2 als Infrastruktur zwischen Kunden/Händler und Bank,

Fig. 3 als optionales hardwarebasierendes Sicherheitssystem,

Fig. 4 als Homebankingserversystem,

Fig. 5 als Prüfelementepoolserversystem,

Fig. 6 als Verfahrensschritt 1, indem ein gesicherter Kanal im Netz aufgebaut wird,

Fig. 7 als Verfahrensschritt 2, indem der Händler als Händler registriert wird,

Fig. 8 als modifizierter Verfahrensschritt 2, indem der Händler über seine Bank einen gesicherten Kanal nutzt,

Fig. 9 als Verfahrensschritt 3, indem der Kunde die Ware/Dienstleistung bestellt und einen Überweisungssatz erhält,

Fig. 10 als Verfahrensschritt 4, indem der Kunde seine Bank zur Zahlung anweist,

Fig. 11 als Verfahrensschritt 5, indem der Kunde die Zahlungsbestätigung erhält,

Fig. 12 als Verfahrensschritt 6, indem der Händler die Zahlungsbestätigung erhält,

Fig. 13 als Verfahrensschritt 7, indem der Händler die Zahlungsbestätigung überprüft und bei Echtheit die Ware/Dienstleistung an den Kunden liefert zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen, dargestellt.

Nach Fig. 1 besteht das Integrationssystem zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen aus dem Kundenrechner 1 des Kunden 2 (einer von beliebig vielen Kunden) mit einem Sicherheitsmodul 3, aus einem Homebankingserver Kundenbank 4, einer Kundenbank EDV 5 der Kundenbank 6 (eine von beliebig vielen Banken), dem Händlerrechner 7 des Händlers 8 (einer von beliebig vielen Händlern) mit dem Sicherheitsmodul 3, optional aus einem Homebankingserver Händlerbank 9, der Händlerbank EDV 10 der Händlerbank 11 (einer von beliebig vielen Banken) und einem Prüfelementepoolserver 12, wobei dieser von dem Händlerrechner 7, der Kundenbank EDV 5 und der Händlerbank EDV 10 über ein Netz 13 erreichbar ist und die Zahlungsanweisungen von dem Händlerrechner 7 über den Kundenrechner 1 an den Homebankingserver Kundenbank 4 in die Kundenbank EDV 5 zur Händlerbank EDV 10 geleitet werden, wobei der Homebankingserver Kundenbank 10 bei einer erfolgreichen Aktion die Bestätigung der Ausführung von der Kundenbank EDV 5 über den Kundenrechner an den Händlerrechner 7 weiterleitet und der Händler 8 die Gültigkeit der Zahlungsanweisung mit Hilfe von Daten aus dem Prüfelementepoolserver 12 selber prüfen und ohne Verzögerung die Waren und Dienstleistungen an den Kunden 2 ausliefern kann.

Nach Fig. 2 ist die Infrastruktur zwischen dem Kunden 2 bzw. Händler 8, der Kundenbank 6 bzw. Händlerbank 11 in der Weise dargestellt, daß der Kundenrechner 1 bzw. der der Händlerrechner 7 zusätzlich zu Sicherheitsmodul 3 eine Nutzerschnittstelle 14 und eine Protokollebene 15 besitzt, wobei eine Verbindung des Kundenrechners 1 bzw. des Händlerrechners 7 über das Netz 13 über den Homebankingserver Kundenbank 4 bzw. optional über den Homebankingserver Händlerbank 9 an die Kundenbank EDV 5 bzw. Händlerbank EDV 10 besteht.

Nach Fig. 3 wird das hardwarebasierende Sicherheitssystem dargestellt, wobei das Sicherheitsmodul 3 als Hardwaresicherheitsmodul 3a aus einem Sicherheitsprotokoll mit Algorithmen 16, aus einer Schlüsselfeldverwaltung 17 dem ein Schlüsselfeld S_{BK} 18 (der Subindex B kennzeichnet die einzelne betrachtete Kundenbank innerhalb der Menge aller Banken, der Subindex K kennzeichnet den einzelnen betrachteten Kunden innerhalb der Menge aller Kunden) nach der Initialisierung zugeordnet ist, aus einer Signaturfeldverwaltung 19, und aus einem Eingabesicherheitsmodul 20, das mit der Tastatur 21 in Wirkverbindung treten kann, besteht.

In der Fig. 4 ist das Homebankingserversystem Kunden/Händlerbank 4; 9 in der Weise angeordnet, daß es aus einem Firewall 22, aus einem Signaturserver 23, aus einem Kommunikationsserver 24, aus einer dynamischen Serverschlüsselfeldverwaltung 25 und einem Protokollserver 26 besteht, wobei der Firewall 22 mit dem Netz 13 sowie mit einem Kommunikationsserver 24 und dem Signaturserver 23 verbunden ist und der Kommunikationsserver 24 mit der Kunden-/Händlerbank EDV 4; 10 sowie mit der dynamischen Serverschlüsselfeldverwaltung 25 verbunden ist, indem die Serverschlüsselfeldverwaltung 25 eine Schlüsselfeldgenerierung 27 beinhaltet, welche die kunden- und bankspezifischen Schlüsselfelder S_{BK} 18 (der Subindex B kennzeichnet die einzelne betrachtete Kundenbank innerhalb der Menge aller Banden, der Subindex K kennzeichnet den einzelnen betrachteten Kunden innerhalb der Menge aller Kunden) sowie der Protokollserver 26 alle auftretenden Datenströme über den Kommunikationsserver 24 protokolliert.

Nach Fig. 5 besteht der Prüfelementepoolserver 12 aus dem Firewall 22, aus dem Kommunikationsserver 24, aus der dynamischen Serverschlüsselfeldverwaltung 25 mit der Schlüsselfeldgenerierung 27, welche die händlerspezifischen Schlüsselfelder S_H 28 (der Subindex H kennzeichnet den einzelnen betrachteten Händler innerhalb der Menge aller Händler) generiert, aus dem Protokollserver 26, dem Bankenprüfelementepool 29 und einem Händlerregistrier- und Verwaltungsmodul 30, indem der Firewall 22 mit dem Netz 13, dem Kommunikationsserver 24 und dem Bankenprüfelementepool 26 Daten austauscht, der Kommunikationsserver 24 mit der dynamischen Serverschlüsselfeldverwaltung 25 sowie mit dem Händlerregistrier- und Verwaltungsmodul 30 verbunden ist und der Protokollserver 26 alle Datenströme über den Kommunikationsserver 24 protokolliert.

In Fig. 6 wird der erste Verfahrensschritt zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen wie folgt dargestellt. Im ersten Verfahrenschritt

wird zwischen dem Homebankingserver Kundenbank 4 der Kundenbank 6 und dem Prüfelementepoolserver 12 ein gesicherter Kanal über das Netz 13 bspw. durch Verschlüsselung 32 aufgebaut. Der Homebankingserver Kundenbank 4 sendet sein Prüfelement (z. B. den Public Key der Bank) P_B 31 (der Subindex B steht für die betrachtete Bank aus der Menge aller Banken) an den Prüfelementepoolserver 12 über den gesicherten Kanal. Somit sind im Prüfelementepool 29 die Prüfelemente P_B 31 (der Subindex B steht für die betrachtete Bank aus der Menge aller Banken) von allen an das System angeschlossenen Banken verfügbar.

Nach Fig. 7 läßt sich im zweiten Verfahrenschritt der Händler 8 beim Prüfelementpoolserver 12 als Händler registrieren und erhält so eine Berechtigung zum Zugriff auf den Prüfelementpoolserver 12, in dem Ihm das händlerspezifische Schlüsselfeld S_H 28 auf einem sicheren Kanal bspw. mittels Verschlüsselung 32 über das Netz 13 zugeführt wird. Mit Hilfe des Schlüsselfeldes S_H ist der Händler 8 in der Lage, einen authentisch verschlüsselten Kanal mit dem Prüfelementepoolserver 12 aufzubauen.

Nach Fig. 8 wird eine modifizierte Variante des zweiten Verfahrensschrittes beschrieben, indem der Händler 8 das händlerspezifische Schlüsselfeld S_H 28, welches ihm den authentischen Zugriff auf den Prüfelementepoolserver 12 erlaubt über eine Bank beantragt. Dabei wird das händlerspezifische Schlüsselfeld S_H 28 in einer nur für den Händler 8 lesbaren Form vom Prüfelementepoolserver 12 auf einem sicheren Kanal bspw. mittels Verschlüsselung 32 über das Netz 13 zum Homebankingserver Kunden-/Händlerbank 4; 9 übertragen und auf einem sicheren Kanal bspw. mittels einer erneuten Verschlüsselung 32 über das Netz 13 zum Händlerrechner 7 des Händlers 8 übertragen. Der Händler 8 speichert das über einen authentischen Kanal von seiner Bank erhaltene händlerspezifische Schlüsselfeld S_H 28 in seinem Hardwaresicherheitsmodul 3a ab.

Nach Fig. 9 nimmt im Verfahrensschritt 3 der Kunde 2 Kontakt bspw. über das Netz 13 mit dem Händler 8 auf, sucht sich eine Ware oder Dienstleistung 33 aus und bestellt diese. Als Antwort auf die Bestellung wird in einem zwischen dem Händler 8 und dem Kunden 2 vereinbarten sicheren Kanal vom Händler ein Überweisungssatz Händler 34 an den Kunden 2 übertagen. Wobei der Überweisungssatz Händler 34 aus Zahlungsinformationen 35, d. h. die Angabe von zahlungsrelevanten Informationen: Bankleitzahl; Kontonummer; Bankinstitut; Name; Betrag + Währung; sonstige Organisationsinformationen, und erweiterte Informationen 36 besteht, in welchem verwaltungs- und produktspezifische Anmerkungen stehen können.

Nach Fig. 10 fügt im 4. Verfahrensschritt der Kunde 2 dem Überweisungssatz Händler 34 mit Hilfe seines Sicherheitsmoduls 3 den komplettierenden Teil der Überweisung als Überweisungssatz Kunde 37 hinzu, so daß eine vollständige Überweisung entsteht. Diese Überweisung wird anschließend über einen sicheren Kanal bspw. mittels Verschlüsselung 32 mittels des bank- und kundenspezifischen Schlüsselfeldes S_{BK} 18 vom Kunden 2 an den Homebankingserver Kundenbank 4 übertragen, auf Vollständigkeit und Auth ntizität überprüft um anschließend weiter an die Kundenbank EDV 5 geleitet zu werden, wo die Abbuchung genehmigt oder abgelehnt wird.

Ist die Entscheidung für die Abbuchung erfolgreich gefällt worden veranlaßt nach Fig. 11 im 5. Verfahrensschritt die Kundenbank 6 die Überweisung an die Händlerbank 11 in den bisher bestehenden Zahlungssystemen an die Händlerbank EDV 10. Gleichzeitig geht von der Kundenbank EDV 5 eine Nachricht an den Homebankingserver Kundenbank 4, daß die Überweisung ausgeführt wird. Nun erzeugt der Homebankingserver Kundenbank 4 einen signierten Bestätigungssatz 38 und überträgt ihn über einen sicheren Kanal, bspw. mittels Verschlüsselung 32 mittels des bank- und kundenspezifischen Schlüsselfeldes S_{BK} 18 über das Netz 13 an dem Kunden 2.

Nach Fig. 12 wird im Verfahrensschritt 6 der Bestätigungssatz 38, welcher aus einer Signatur 39, welche bankspezifisch ist, Zahlungsinformationen 35, d. h. Organisisationsinformation, Bankidentifikation, Überweisungszeitpunkt, Datum, Betrag + Währung, und erweiterten Informationen 36 besteht, vom Kunden 2 über einen beliebigen vereinbarten Kanal bspw. über das Netz 13 an den Händler 8 übertragen.

Nach Fig. 13 überprüft im 7. Verfahrensschritt der Händler 8 die Signatur 39 des Bestätigungssatzes 38 indem die Signatur 39 eine Funktion des Bestätigungssatzes 38 und des bankspezifischen Prüfelementes P_B 31 ist, indem der Händler 8 das bankspezifische Prüfelement P_B 31 aus seinem Speicher oder optional authentisch über einen sichern Kanal bspw. mittels Verschlüsselung 32 mittels des händlerspezifischen Schlüsselfeldes S_H 28 vom Prüfelementepoolserver 12 bezieht und die Signatur 39 auf Echtheit überprüft. Ist diese Überprüfung korrekt, veranlaßt der Händler 8 die Überweisung der Ware-Dienstleistung 33 an den Kunden 2, womit das Verfahren zur Abwicklung des Zahlungsverkehrs über Netze beendet ist.

Die erfindungsgemäße Lösung ist dadurch charakterisiert, daß einzelne Nutzer im Handelssystem, also der Kunde 2 und der Händler 3 gewisse infrastrukturelle Voraussetzungen erfüllen müssen, um an dem Handelssystem teilzunehmen. Um die Funktion des Kaufens und Verkaufens gegenüber dem Kunden 2 abzuwickeln, wird auf dem Kundenrechner 1 eine Nutzerschnittstelle 14 benötigt. Diese kann auf verschiedenste Weise ausgeführt sein. Entweder als eigenständiges Programm oder als Teil eines andern Programmes z. B. eines Browsers. Dabei kann die Nutzerschnittstelle 14 grafisch gestaltet sein, in dem bspw. das Geld durch kleine Geldsacksymbole dargestellt und die Zahlung durch eine Bewegung eines dieser Symbole auf eine "Landefläche" aktiviert wird. Nach dieser Absichtserklärung zur Ausführung eines Zahlungsprozesses wird der eigentliche Zahlungsvorgang gestartet. Die vielfältigen Möglichkeiten, welche der Kunde zum Starten eines Zahlungsprozesses durch eine grafische Schnittstelle hat, sollen hier nicht weiter ausgeführt werden.

Neben der Nutzerschnittstelle 14 ist in jedem System eine Protokollebene 15 integriert, die die verschiedenen später dargestellten Prozesse abwickelt und koordiniert, so daß der Kunde nur die minimalen Aktionen vollführen muß.

Das Sicherheitsmodul 3 ist eines der wesentlichen Bestandteile der Lösung. Dabei kann sowohl ein Softwaresicherheitsmodul 3b, als auch ein Hardwaresicherheitsmodul 3a verwandt werden. Die maximale Sicherheit vor digitalen Angriffen kann nur durch ein Hardwaresicherheitsmodul 3a erreicht werden.

Der Kundenrechner 1 oder Händlerrechner 7 ist mit einem Netz 13 oder über eine direkte Telefonleitung miteinander verbunden. Insbesondere sollen hier inhomogene Netze betrachtet werden, wie bspw. das Internet. Direkt am Netz 13 (Internet) ist auch der Home-

bankingserver Kundenbank 4 bzw. optional der Homebankingserver Händlerbank 9 angeschlossen, der die ankommenden Daten in die Kundenbank EDV 5 bzw. Händlerbank EDV 10 leitet. Die Kundenbank 6 muß eine Möglichkeit für Online-Transaktion für den Kunden bieten. Die Händlerbank 11 hingegen muß nicht onlinefähig sein.

Als ein Realisierungsbeispiel soll anhand des Hardwaresicherheitsmoduls 3a die Funktion der Sicherheit des Systems erläutert werden. Innerhalb des Hardwaresicherheitsmoduls 3a, wobei es sich um einen einzelnen Schaltkreis oder um eine Chipkarte handeln kann, sind nachfolgende wesentlichen funktionellen Elemente untergebracht, die in verschiedenen technischen Formen realisiert werden können (als Microcode, als fest verdrahtete Schaltung oder als programmierbare Struktur usw.). Jedes Hardwaresicherheitsmodul 3a kann eine einmalige Nummer beherbergen oder andere selektivierende Kriterien erhalten.

Das Sicherheitsprotokoll mit Algorithmen 16 beinhaltet die Algorithmen zur Ver- und Entschlüsselung. Bspw. können sowohl symmetrisch als auch asymmetrisch Algorithmen verwandt werden. Wesentliche protokollspezifische Funktionen werden ebenfalls in dieser Einheit abgewickelt (Schlüssellänge einstellen usw.).

In der Schlüsselfeldverwaltung 17 wird der Grundstein für eine sicher Kommunikation mit der Kundenbank 61 Händlerbank 11 gelegt, wobei hier verschieden Funktionen ausgeführt werden können. Die im folgenden beschriebene Funktion stellt nur ein Beispiel dar und soll die technische Machbarkeit aufzeigen. Das erwünschte Ergebnis kann jedoch technisch auch auf andere Weise erzeugt werden.

Beim Ausgeben der einzelnen Hardwaresicherheitsmodule 3a, befinden sich Initalschlüsselfelder in der Schlüsselfeldverwaltung 17. Für jedes Hardwaresicherheitsmodul 3a ist ein anderes Schlüsselfeld festgelegt. Diese Initialschlüsselfelder sind der Kundenbank 6/Händlerbank 11 oder einer dritten Organisation bekannt. Bei dem ersten Kontakt wird das Initialschlüsselfeld durch das kunden- und bankspezifische Schlüsselfeld S_{BK} 18 ersetzt bzw. parallel dazu in den Chip geladen. Damit kann eine sichere Kommunikation zur Kundenbank 6/Händlerbank 11 aufgebaut werden, in dem jeder ankommende Transaktionsschlüssel mit dem Schlüsselfeld der Bank umgeschlüsselt wird und erst dann im Hardwaresicherheitsmodul 3a mit Hilfe dieses umgeschlüsselten Schlüssels die Informationen ver- oder entschlüsselt werden. Verschiedene Banken können Ihre Schlüsselfelder in das Sicherheitsmodul 3 portieren, die in der Schlüsselfeldverwaltung 17 gespeichert werden.

In derselben Art und Weise können die Schlüsselfelder für Signaturen in das Hardwaresicherheitsmodul 3a geladen werden. Diese Signaturfunktionen sind wichtig im Zusammenhang mit dem Eingabesicherheitsmodul 20. Das Eingabesicherheitsmodul 20 garantiert für die Richtigkeit der Eingabe sowie dafür, daß von der Eingabe bis zum Sicherheitsmodul 3 keine Manipulationen an den Daten erfolgen. Dies geschieht bspw. indem die Tastatur 21 direkt mit dem Eingabesicherungsmodul 20 verbunden ist und so keine Manipulationen der Eingabe möglich sind.

Das Homebankingserversystem bildet die Verbindung von der spezifischen Bank EDV 5/10 zum Netz 13. Dabei kann das System verschiedensten Anforderungen gerecht werden. Vorrangig muß natürlich die Sicherheit der spezifischen Bank EDV 5/10 gewährleistet werden. Es gibt verschiedenste Möglichkeiten, die Anforderungen an ein Homebankingsystem zu erfüllen, hier soll nur ein Beispiel erläutert werden.

Alle aus dem Netz 13 ankommenden Daten werden über den Firewall 22 auf Unversehrtheit, Authentizität usw. geprüft. Dies geschieht bspw. indem direkt auf die Netzwerkkarte zugegriffen wird und die Datenpakete direkt von der Hardware gelesen werden um anschließend zu überprüfen, ob diese Daten mit einem Sicherheitsmodul 3 verschlüsselt wurden oder nicht. Im nächsten Schritt wird überprüft, ob es sich dabei um Sicherheitsmodule 3 handelt, die in der dynamischen Serverfeldschlüsselverwaltung 25 gespeichert sind. Nur wenn auch diese Prüfung positiv abgelaufen ist, werden die Daten akzeptiert und an den Kommunikationsserver 26 weitergeleitet, welcher den Datensatz entschlüsselt und die Signatur 39 auf Gültigkeit überprüft. In der dynamischen Serverschlüsselfeldverwaltung 25 werden die von diesem Homebankingserver Kundenbank 4 erzeugten verschiedenen Schlüsselfelder S_{BK} 18 (der Subindex B kennzeichnet die einzelne betrachtete Kundenbank 6 innerhalb der Menge aller Banken, der Subindex K kennzeichnet den einzelnen betrachteten Kunden 2 innerhalb der Menge aller Kunden 2) für alle Kunden gespeichert und bei Bedarf zur Verfügung gestellt. Der Signaturserver 23 erzeugt die einzelnen notwendigen Schlüssel für die Kundenbank 6 und den Kunden 2 um die einzelnen elektronischen Signaturen 39 zu erzeugen und zu prüfen. Der Kommunikationsserver 24 ist für die gesamte Kommunikation zur Kundenbank EDV 6 hin zuständig und für die eigentliche Ver- und Entschlüsselung der Datenströme. Dabei emuliert der Kommunikationsserver 24 das benötigte Protokoll für die Kundenbank EDV 6 da es sich hierbei um Systeme handelt, die nur mit sehr hohen Kosten geändert werden können. Jede Transaktion und alle relevanten Prozesse werden von dem Protokollserver 26 mitgeschreiben und stehen so bei eventuell auftretenden Fehlern zur Überprüfung bereit.

Um den einzelnen an das System angeschlossenen Kunden 2/Händlern 8, eine einfache Möglichkeit zur Prüfung der Echtheit der einzelnen Aktionen zu gewährleisten, muß ein authentischer Kanal geschaffen werden um die Prüfelemente P_B 31 zu übertragen. In dem beschriebenen Ausführungsbeispiel, sind die Prüfelemente P_B 31 die Publik Keys der Banken. Diese Publik Keys sind nicht geheim, sollten aber über einen authentischen Kanal für den Händler 8 beschaffbar sein. Gleichzeitig kann jeder Kunde 2 einfach zum Händler 8 werden, indem er sich am Prüfelementepoolserver 12 meldet und mit Hilfe des Händlerregistrier- und Verwaltungsmoduls 30 anhand der Nummer seines Sicherheitsmoduls 3 identifiziert wird. Nach dem er als Händler 8 zugelassen wurde wird in der dynamischen Schlüsselfeldverwaltung 25 ein händlerspezifisches Schlüsselfeld S_H 28 (der Subindex H kennzeichnet den einzelnen betrachteten Händler 8 innerhalb der Menge aller Händler 8) kreiert, um später in sein Sicherheitsmodul 3 geladen zu werden. Wenn der Händler 8 später eine Bestätigung für eine getätigte Aktion des Kunden 2 oder seiner Kundenbank 6/Händlerbank 11 überprüfen möchte, so muß er mit dem erhaltenen Schlüsselfeld S_H 28 den Prüfelementepoolserver 12 kontaktieren und er erhält aus dem Prüfelementepoll 29 das entsprechende Prüfelement (z. B.: den Public Key der Bank) P_B 31 (der Subindex B steht für die betrachtete Kundenbank 6 aus der Menge aller Banken) mit dessen Hilfe er die Echtheit der Bestätigung vom Kunden 2 über den Zahlungsvollzug über-

prüfen kann. Alle anderen Elemente üben die selben Funktionen aus, wie im Homebankingserversystem bereits beschrieben.

Der Aufbau eines gesicherten Kanals kann bspw. derart ausgeführt werden, in dem im Homebankingserversystem ein Private Key/Public Key Schlüsselpaar erzeugt wird, welches später zur Erzeugung von Signaturen 39 verwandt wird. Dabei muß jedoch der bank- und kundenspezifische Public Key dem späteren Partner über einen authentischen Kanal zugeführt werden, damit dieser die Echtheit der Signatur 39 vor Ort prüfen kann. Deshalb wird der Public Key über einen gesicherten Kanal an den Prüfelementepoolserver 12 übertragen und dort abgespeichert. Im Prüfelementepoolserver 12 sind somit alle Public Keys der Kundenbanken 6 zuordenbar abgespeichert.

Im nachfolgenden Ausführungsbeispiel wird gezeigt, wie der Händler 8 registriert wird. Das erfolgt in der Weise, daß im Hardwaresicherheitsmodul 3a vorvereinbarte Initialschlüsselfelder existieren, welche dem Prüfelementepoolserver 12 oder der Händlerbank 11 bekannt sind, mit dessen Hilfe der Händler 8 den ersten Kontakt zum Prüfelementepoolserver 12 aufbauen kann, nachdem er erfolgreich als Händler 8 registriert wurde. Ist die erforderliche Prüfung zur Zulassung als Händler 8 (wirtschaftliche Prüfung, Zulassung ect.) erfolgreich abgelaufen, wird über diesen sicheren Kanal bspw. mittels Verschlüsselung 32 über das Netz 13 dem Händler 8 ein entsprechendes händlerspezifisches Schlüsselfeld S_H 28 übertragen, mit dessen Hilfe er in Zukunft auf das Prüfelement (z. B. den Public Key) P_B 31 einer im System teilnehmenden Kundenbank 6 über den Prüfelementepoolserver 12 sicher und authentisch zugreifen kann. Als Anwendungsbeispiel für eine modifizierte Variante kann der Händler 8, falls seine Händlerbank 11 auch einen Homebankingserver Händlerbank 9 besitzt, was nicht unbedingt zur Abwicklung des Verfahrens notwendig ist, die Berechtigung und das händlerspezifische Schlüsselfeld S_H 28 von seiner Händlerbank 11 erhalten, indem die Händlerbank 11, mit Hilfe ihres Homebankingservers Händlerbank 9, über den selben Kanal, mit welchem die Prüfelemente P_B 31 gesichert an den Prüfelementepoolserver 12 übertragen wurden, den Prüfelementepoolserver 12 kontaktiert und das entsprechende händlerspezifische Schlüsselfeld S_H 28 zur sicheren Kontaktausfnahme für den Händler 8 bezieht und seinerseits dieses an den Händler 8 über den gesicherten Kanal zwischen Händler 8 und dem Homebankingserver Händlerbank 9 überträgt.

Als Anwendungsbeispiel kann der Kunde 2 im Internet über WEB Pages das Angebot des Händlers 8 betrachten und sich ein ihn interessierendes Produkt aussuchen. Nach der Auswahl, wird zwischen dem Händler 8 und dem Kunden 2 über ein beliebiges bestehendes Softwaresicherheitsprotokoll (bspw. SSL usw.) ein sicherer Kanal aufgebaut, in dem ein vorausgefüllter Überweisungssatz Händler 34 mit Zahlungsinformationen 35 und erweiterten Informationen 36 die später in der Händlerbank EDV 10 für die Zuordnung der Überweisung eine vereinfachende Rolle spielen werden, übertragen wird.

Die Zahlungsanweisung des Kunden 2 an den Händler 8 kann sehr einfach und sicher für den Kunden 2 gestaltet werden, indem bspw. durch einen einfachen Mausklick das zu belastende Konto dem vom Händler 8 ausgestellten Überw isungssatz Händler 34 hinzugefügt wird und nur noch der Betrag über die Tastatur 21 direkt in das Sicherheitsmodul 3 eingegeben werden muß. Indem der Kunde 2 den Betrag erneut eingegeben hat ist sichergestellt, daß die Überweisung vom Kunden 2 genehmigt wurde. Nachdem die Überweisung mit Empfänger und Adressat vollständig vorliegt, kann diese verschlüsselt und signiert werden, um dann über den sicheren Kanal zwischen der Kundenbank 6 und dem Kunden 2 übertragen zu werden. Im Homebankingserver Kundenbank 4 wird die Überweisung nach der Entschlüsselung und der Überprüfung der Echtheit der Überweisung entsprechend der Syntax der speziellen Kundenbank EDV 5 umgerechnet und optional ergänzt an die Kundenbank EDV 5 übertragen. In dieser kann anschließend entscheiden werden, ob der Kunde 2 über den zu überweisenden Betrag verfügen kann. Optional kann diese Entscheidung auch in dem Homebankingserver Kundenbank 9 getroffen werden, falls entsprechende Angaben über den Kunden 2 im System vorliegen oder von der Kundenbank EDV 5 abgefragt werden können.

Nach der Überweisung durch die Kundenbank EDV 5 kann die bestehende Händlerbank EDV 10 die Überweisungssätze der Händlerbank 11 einlesen und in bewährter Art und Weise in ihrem Verwaltungssystem nutzen.

Die Überprüfung des Bestätigungssatzes 38 vom Händler 8 erfolgt in der Weise, indem der Händler 8 die Signatur 39 des Bestätigungssatzes 38 durch das Prüfelement (Public Key) P_B 31 der Bank überprüft. Für häufiger genutzte Institute (große Banken) wird er in der Regel die Prüfelemente (Public Keys) P_B 31 schon auf seinem Händlerrechner 7 haben. Damit braucht er nur dann Kontakt mit dem Prüfelementepoolserver 12 aufnehmen, wenn ein Kunde 8 von einer Kundenbank 6 zahlt, deren Prüfelement (Public Key) P_B 31 noch nicht beim Händler 8 gespeichert ist.

Das beschriebene Verfahren zur Integration von Kunden 2 und Händlern 8 innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze 13 ist nicht auf Banken beschränkt. An die Stelle der Kundenbank 4 und/oder der Händlerbank 11 können beliebige Finanzdienstleister treten, mit denen ähnliche Prozesse im Zahlungsverkehr abgewickelt werden.

Verwendete Abkürzungen

VISA Handelsname
MASTERCARD Handelsname
SET-Protokoll secure-electronic-transaction-protocoll
DIGICASH Handelsname
RSA Revest-Sharmir-Adelman Verschlüsselungsalgorithmus
DEBIT Handelsname
WWW-Pages world wide web pages
SSL security-socet-layer

Bezugszeichenliste

1 Kundenrechner
2 Kunde
3 Sicherheitsmodul
3a Hardwaresicherheitsmodul
3b Softwaresicherheitsmodul
4 Homebankingserver Kundenbank
5 Kundenbank EDV
6 Kundenbank
7 Händlerrechner
8 Händler

9 Homebankingserver Händlerbank
10 Händlerbank EDV
11 Händlerbank
12 Prüfelementepoolserver
13 Netz
14 Nutzerschnittstelle
15 Protokollebene
16 Sicherheitsprotokoll mit Algorithmen
17 Schlüsselfeldverwaltung
18 S_{BK} (bank-und kundenspezifisches Schlüsselfeld)
19 Signaturfeldverwaltung
20 Eingabesicherheitsmodul
21 Tastatur
22 Firewall
23 Signaturserver
24 Kommunikationsserver
25 Dynamische Serverschlüsselfeldverwaltung
26 Protokollserver
27 Schlüsselfeldgenerierung
28 S_H (händlerspezifisches Schlüsselfeld)
29 Prüfelementepool
30 Händlerregistrier- und Verwaltungsmodul
31 P_B (bankspezifisches Prüfelement)
32 Verschlüsselung
33 Ware Dienstleistung
34 Überweisungssatz Händler
35 Zahlungsinformationen
36 erweiterte Informationen
37 Überweisungssatz Kunde
38 Bestätigungssatz
39 Signatur

Patentansprüche

1. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze, indem die Kunden mittels ihres Kundenrechners den Zahlungsverkehr über Netzwerke mit ihrer speziellen Bank EDV abwickeln, **dadurch gekennzeichnet,** daß ein Prüfelementepoolserver (12) das bankspezifische Prüfelement P_B (31) der Kundenbank (6) authentisch einem Händler (8) sicher zur Verfügung stellt, welcher dadurch die erfolgreiche Abwicklung des Zahlungsverkehrs zwischen der Kundenbank (6) und der Händlerbank (11) kontrollieren kann, ohne das der Händler (8) einen Kontakt zu Händlerbank (11) aufnehmen muß, indem der Prüfelementepoolserver (12) im Prüfelementepool (29) die bankspezifischen Prüfelemente P_B (31) der Banken gespeichert und auf Anforderung über einen sicheren Kanal dem Händler (8) zur Verfügung stellt, indem eine sichere Verbindung zwischen dem Prüfelementepoolserver (12) und dem Händler (8) über ein Netz (13) realisiert wird, indem die Verbindung zwischen dem Kunden (2) und der Kundenbank (6) über ein Sicherheitsmodul (3) und dem Homebankingserver Kundenbank (4) abgewickelt wird, wobei der Homebankingserver Kundenbank (4) sowohl den Datenverkehr mit dem Prüfelementepoolserver (12) als auch mit der bestehenden Kundenbank EDV (5) abgewickelt, ohne daß Änderungen an der Kundenbank EDV (5) vorgenommen werden müssen.

2. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 dadurch gekennzeichnet,

daß

im 1. Verfahrenschritt

jeder Homebankingserver Kundenbank (4) über einen gesicherten Kanal (z. B. durch Verschlüsselung 32) zwischen dem Homebankingserver Kundenbank (4) und dem Prüfelementepoolserver (12) sein bankspezifisches Prüfelement P_B (31) an den Prüfelementepoolserver (12) sendet, so daß von allen an das System angeschlossenen Kundenbanken (6) die bankspezifischen Prüfelemente P_B (31) im Prüfelementepool (29) des Prüfelementepoolservers (12) authentisch verfügbar sind,

im 2. Verfahrensschritt

der Händler (8) sich beim Prüfelementepoolserver (12) als Händler (8) registrieren läßt, und einen sicheren Kanal etabliert und somit eine authentische Zugriffsberechtigung auf den Prüfelementepoolserver (12) mit dem Prüfelementepool (29) erhält,

im 3. Verfahrensschritt

der Kunde (2) mit dem Händler (8) über das Netz (13) Kontakt aufnimmt, sich eine Ware Dienstleistung (33) auswählt und bestellt, indem als Antwort auf die Bestellung in einem zwischen dem Händler (8) und dem Kunden (2) vereinbarten sicheren Kanal vom Händler (8) einen Überweisungssatz Händler (34) an den Kunden (2) übertragen wird, wobei der Überweisungssatz Händler (34) aus Zahlungsinfoimationen (35) und erweiterten Informationen (36), in welchem verwaltungs- und produktspezifische Anmerkungen stehen, besteht,

im 4. Verfahrensschritt

der Kunde (2) die Überweisung an den Händler (8) vornimmt, indem er mit Hilfe seines Sicherheitsmoduls (3) den Überweisungssatz Händler (34) komplettiert, indem er einen Überweisungssatz Kunde (37) erstellt, so daß eine vollständige Überweisung entsteht, diese über einen sicheren Kanal vom Kundenrechner (1) über den Homebankingserver Kundenbank (4) an die Kundenbank EDV (5) der Kundenbank (6) überträgt, wo die Überweisung genehmigt oder abgelehnt wird,

im 5. Verfahrensschritt

nach erfolgreicher Überweisung der Kundenbank (6) an die Händlerbank (11) über bestehende Zahlungsstrukturen von der Kundenbank EDV (5) der eine Nachricht an den Homebankingserver Kundenbank (4) ausgeht, der Homebankingserver Kundenbank (4) einen Bestätigungssatz (38) generiert und auf dem sicheren Kanal zwischen dem Kunden (2) und dem Homebankingserver (4) an den Kunden (2) überträgt,

im 6. Verfahrensschritt

der Kunde (2) den Bestätigungssatz (38) und über einen beliebig mit dem Händler (8) vereinbarten Kanal an den Händler (8) überträgt,

im 7. Verfahrensschritt

der Händler (8) den Bestätigungssatz (38) auf seine Echtheit überprüft und bei Echtheit die Ware Dienstleistung (33) an den Kunden (2) liefert, indem er den Bestätigungssatz (38) mit Hilfe des bankspezifischen Prüfelementes P_B (31) überprüft, indem er eine sichere Verbindung zum Prüfelementepoolserver (12) herstellt und sich das authentische bankspezifische Prüfelement P_B (31) in den Händlerrechner (5) überträgt, falls er das Prüfelement P_B (31) nicht schon auf seinem Rechner besitzt, und bei erfolgreicher Überprüfung die Ware Dienstleistung (33) freigibt,

im 8. Verfahrensschritt
wenn die Überweisung von der Kundenbank (6) erfolgt ist, kann die Händlerbank EDV (10) wie bisher die Überweisungssätze von der Händlerbank (11) einlesen und in ihrem Verwaltungssystem nutzen.

3. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im 1. Verfahrensschritt zur Generierung des bank- und kundenspezifischen Schlüsselfelder S_{BK} (18) und des bankspezifischen Prüfelementes P_B (31) im Homebankingserver Kundenbank (4) ein Private Key/Public Key Schlüsselpaar erzeugt wird, welches später zur Erzeugung von Signaturen (39) verwandt wird, indem der Public Key dem Prüfelementepoolserver (12) über einen authentischen Kanal zugeführt und zusammen mit den Public Keys anderer Kundenbanken (6) zuordenbar im Prüfelementepool (29) abgespeichert wird.

4. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung dem Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im 2. Verfahrensschritt der Händler (8) das händlerspezifische Schlüsselfeld S_H (28), welches ihm den authentischen Zugriff auf den Prüfelementepoolserver (12) erlaubt, über seine Händlerbank (11) beantragt, indem dieses händlerspezifische Schlüsselfeld S_H (28) vom Prüfelementepoolserver (12) in einer spezifisch nur für den Händler (8) lesbaren Form in den Homebankingserver Händlerbank (9) übertragen und in diesem, erneut verschlüsselt, über den sicheren Kanal zwischen dem Händler (8) und dem Homebankingserver Händlerbank (9) der Händlerbank (11) übertragen wird.

5. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im zweiten Verfahrenschritt, das händlerspezifische Schlüsselfeld S_H (28) für den authentischen Zugriff des Händlers (8) zum Prüfelementepoolserver (12) über einen sicheren Kanal zwischen dem Prüfelementepoolserver (12) und dem Händler (8) übermittelt wird, indem für den Erstkontakt ein im Sicherheitsmodul (3) des Händlers (8) vereinbartes spezielles Initialschlüsselfeld als Defaultschlüsselfeld verwendet wird, welches nach erfolgreicher Anmeldung als Händler (8) mit dem eigentlichen händlerspezifischen Schlüsselfeld S_H (28) überschrieben werden kann.

6. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im 3. Verfahrensschritt der Kunde (2) im Netz über WWW Pages das Angebot des Händlers (8) betrachten und sich eine ihn interessierende Ware Dienstleistung (33) Online aussuchen und bestellen kann.

7. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch

gekennzeichnet, daß im 3. Verfahrensschritt die Zahlungsinformation (35) unterscheidliche zahlungsrelevante Informationen, also Angaben über Bankleitzahl, Bankinstitut, Kontonummer, Name, Betrag, Währung und sonstige Organisationsinformationen enthält.

8. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im 4. Verfahrensschritt der Überweisungsprozeß durch die Nutzerschnittstelle (14) softwaremäßig für den Kunden (2) sehr einfach und sicher gestaltet ist, indem durch einen einfachen Mausklick dem vom Händler (8) ausgestellten Überweisungssatz Händler (34) das zu belastende Konto hinzugefügt werden kann und nur noch der Betrag über die Tastatur (21) direkt in das Sicherheitsmodul (3) eingegeben werden muß, wodurch sichergestellt ist, daß die Überweisung vom Kunden (2) genehmigt wurde, da er den Betrag erneut eingegeben hat.

9. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß im 4. Verfahrensschritt die Entscheidung über die Genehmigung/Ablehnung der Überweisung direkt im Homebankingserver Kundenbank (4) getroffen wird, indem entsprechende Angaben über den Kunden (2) im System vorliegen oder von der Kundenbank EDV (5) abgefragt werden können.

10. Verfahren zur Integration von Kunden und Händlern innerhalb bestehender Zahlungsstrukturen bei der Abwicklung des Zahlungsverkehrs über Netze nach Anspruch 1 und Anspruch 2 dadurch gekennzeichnet, daß an die Stelle von der Kundenbank (4) und/oder der Händlerbank (11) beliebige Finanzdienstleister treten können, mit denen ähnliche Prozesse im Zahlungsverkehr abgewickelt werden.

11. Anordnung zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen dadurch gekennzeichnet, daß im Ausführungsbeispiel ein Integrationssystem aus dem Kundenrechner (1) mit einem Sicherheitsmodul (3), welches als Hardwaresicherheitsmodul (3a) oder Softwaresicherheitsmodul (3b) ausgeführt ist, aus einem Homebankingserver Kundenbank (4), einer Kundenbank EDV (5), dem Händlerrechner (7) mit dem Sicherheitsmodul (3) optional aus einem Homebankingserver Händlerbank (9), der Händlerbank EDV (10) und einem Prüfelementepoolserver (12) besteht, wobei dieser von dem Händlerrechner (7), dem Homebankingserver Kundenbank (4) und optional dem Homebankingserver Händlerbank (9) über ein Netz (13) erreichbar ist.

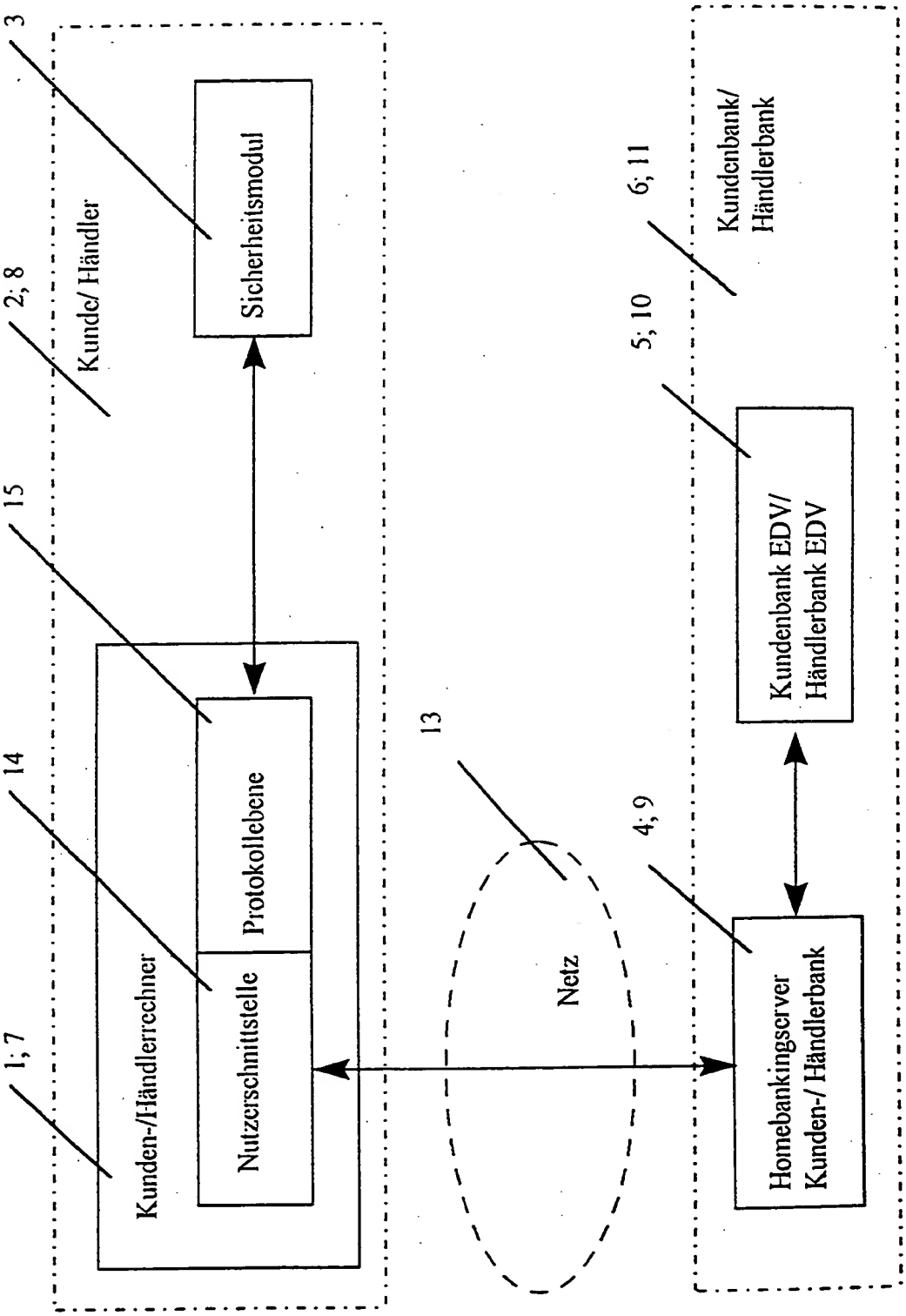
12. Anordnung zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen nach Anspruch 11 dadurch gekennzeichnet, daß das Sicherheitsmodul (3) ein spezielles Hardwaresicherheitsmodul (3a) mit selektivierenden Kriterien ist, bestehend aus einem Sicherheitsprotokoll mit Algorithmen (16), einer Schlüsselfeldverwaltung (17), dem ein bank- und kundenspezifisches Schlüsselfeld S_{BK} (18) nach der Initialisierung zugeordnet ist, einer Signaturfeldverwaltung (19), sowie aus einem Ein-

gabesicherungsmodul (20), das mit der Tastatur (21) in Wirkverbindung treten kann, wodurch der Informationsfluß von der Tastatur (21) bis zur Verschlüsselung (32) in einer geschlossenen Umgebung realisiert wird.

13. Anordnung zur Abwicklung von kostengünstigen Zahlungen auf digitalen Netzen nach Anspruch 11 dadurch gekennzeichnet, daß der Prüfelementepoolserver (12) aus dem Firewall (22), dem Kommunikationsserver (24), der dynamischen Serverschlüsselfeldverwaltung (25) mit der Schlüsselfeldgenerierung (27) den händlerspezifischen Schlüssel S_H (28) dem Protokollserver (26), dem Prüfelementepool (29) und einem Händlerregistrier- und Verwaltungsmodul (30) besteht, indem der Firewall (22) mit dem Kommunikationsserver (24) verbunden ist und über das Netz (13) Daten austauscht, daß der Kommunikationsserver (24) mit der dynamischen Serverschlüsselfeldverwaltung (25) mit der Schlüsselfeldgenerierung (27) sowie mit dem Händlerregistrier- und Verwaltungsmodul (30) verbunden ist und der Protokollserver (26) alle Datenströme über den Kommunikationsserver (24) protokolliert.

Hierzu 13 Seite(n) Zeichnungen

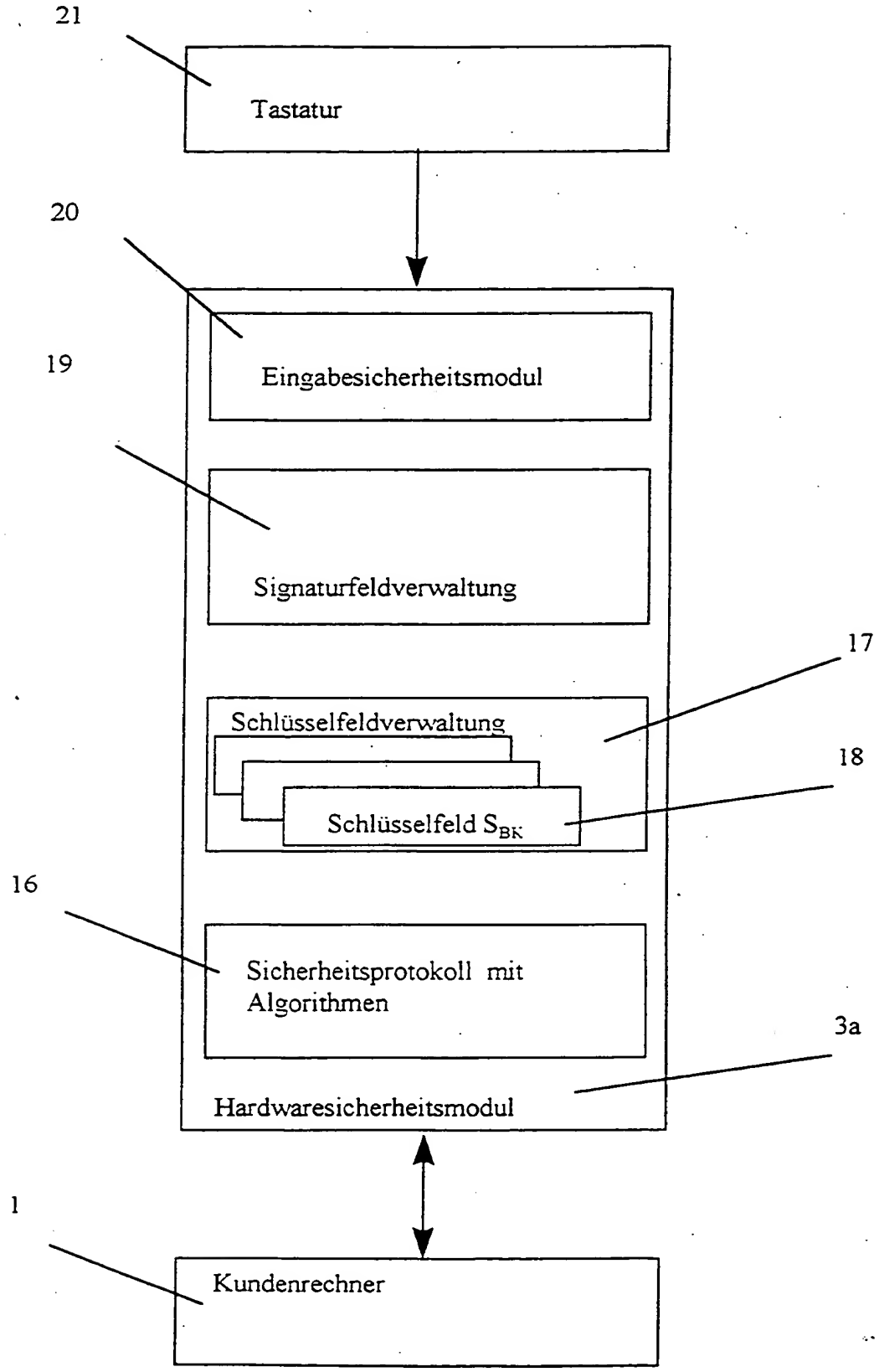
Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



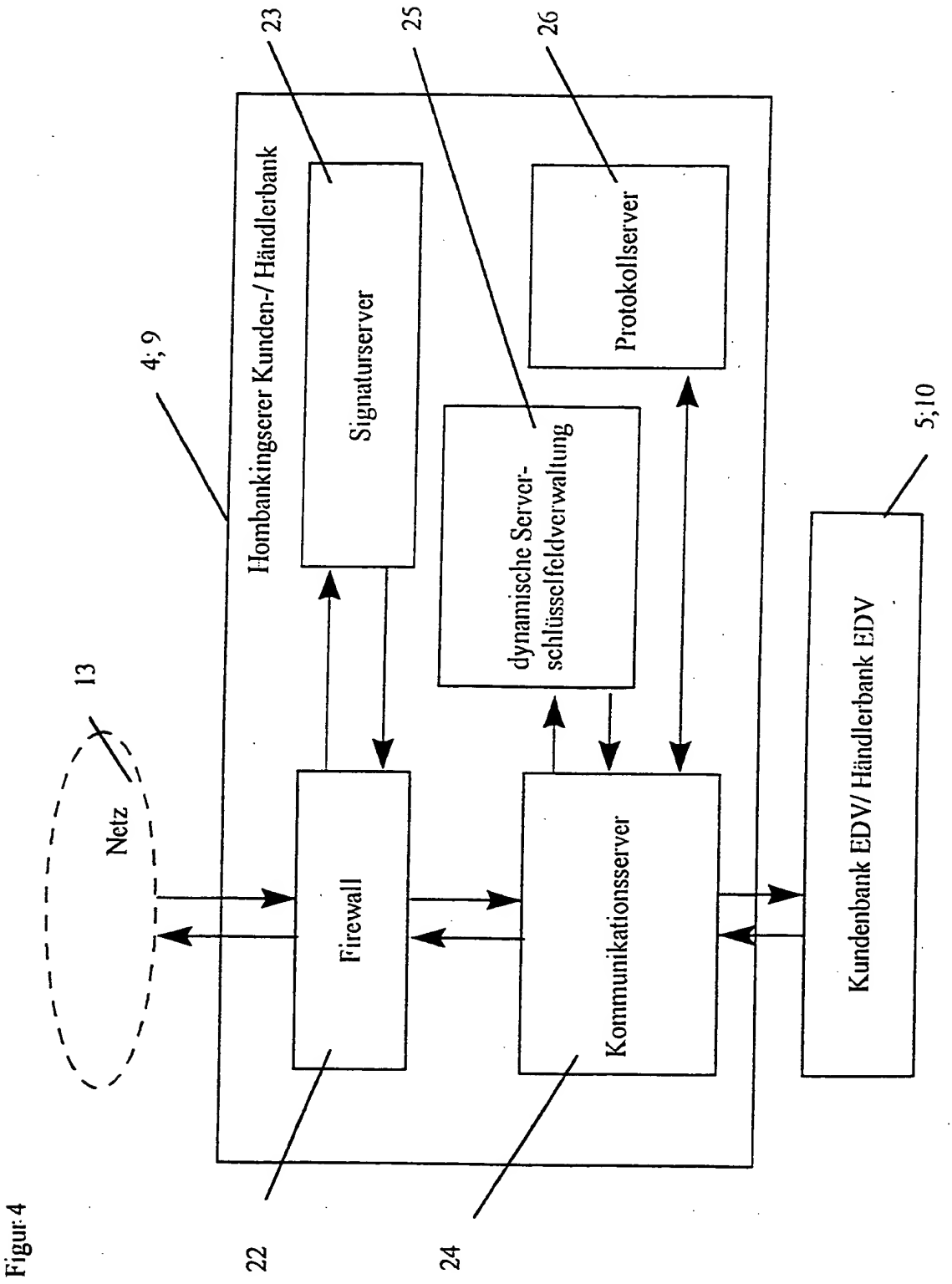
Figur 2

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998

Figur 3

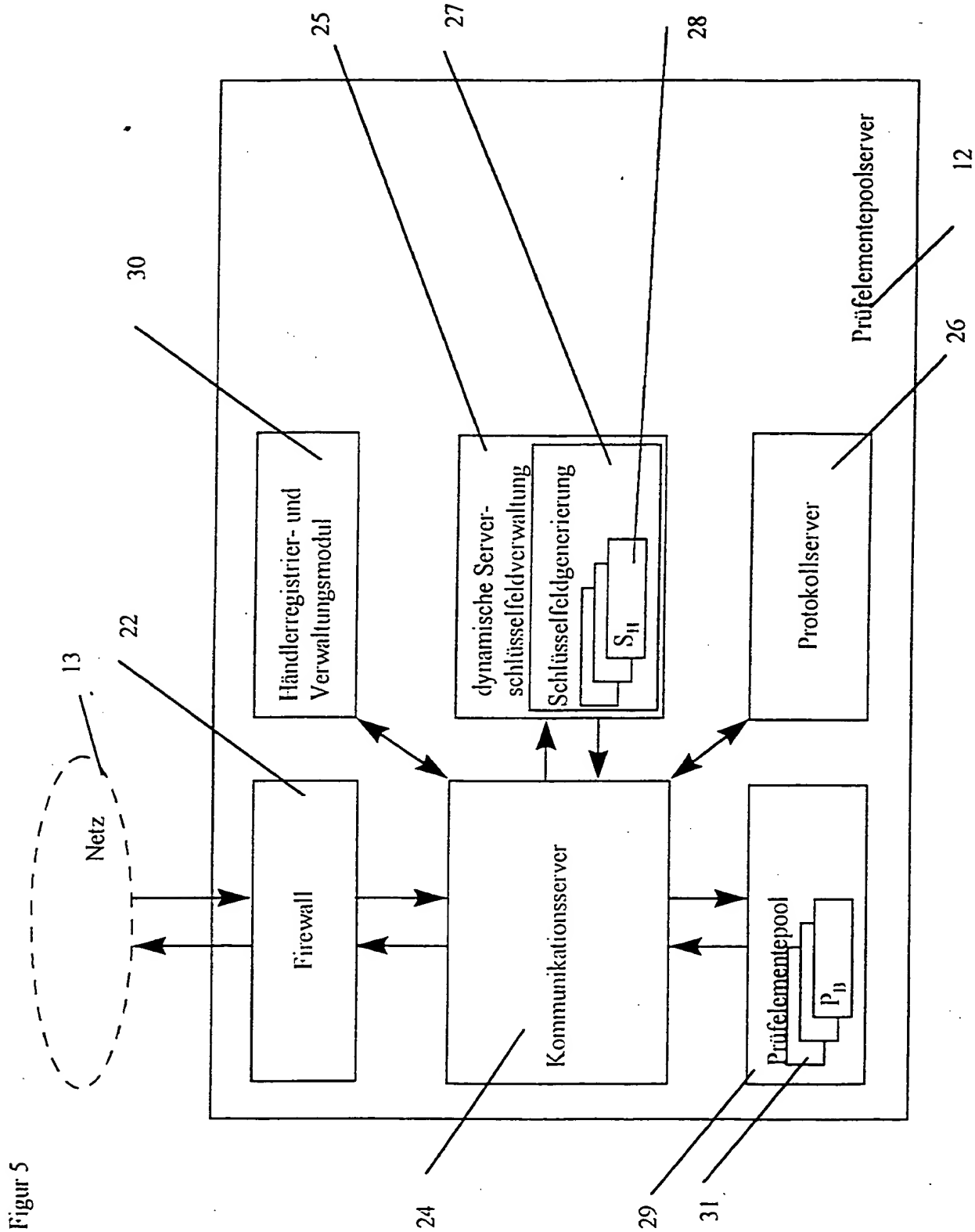


Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



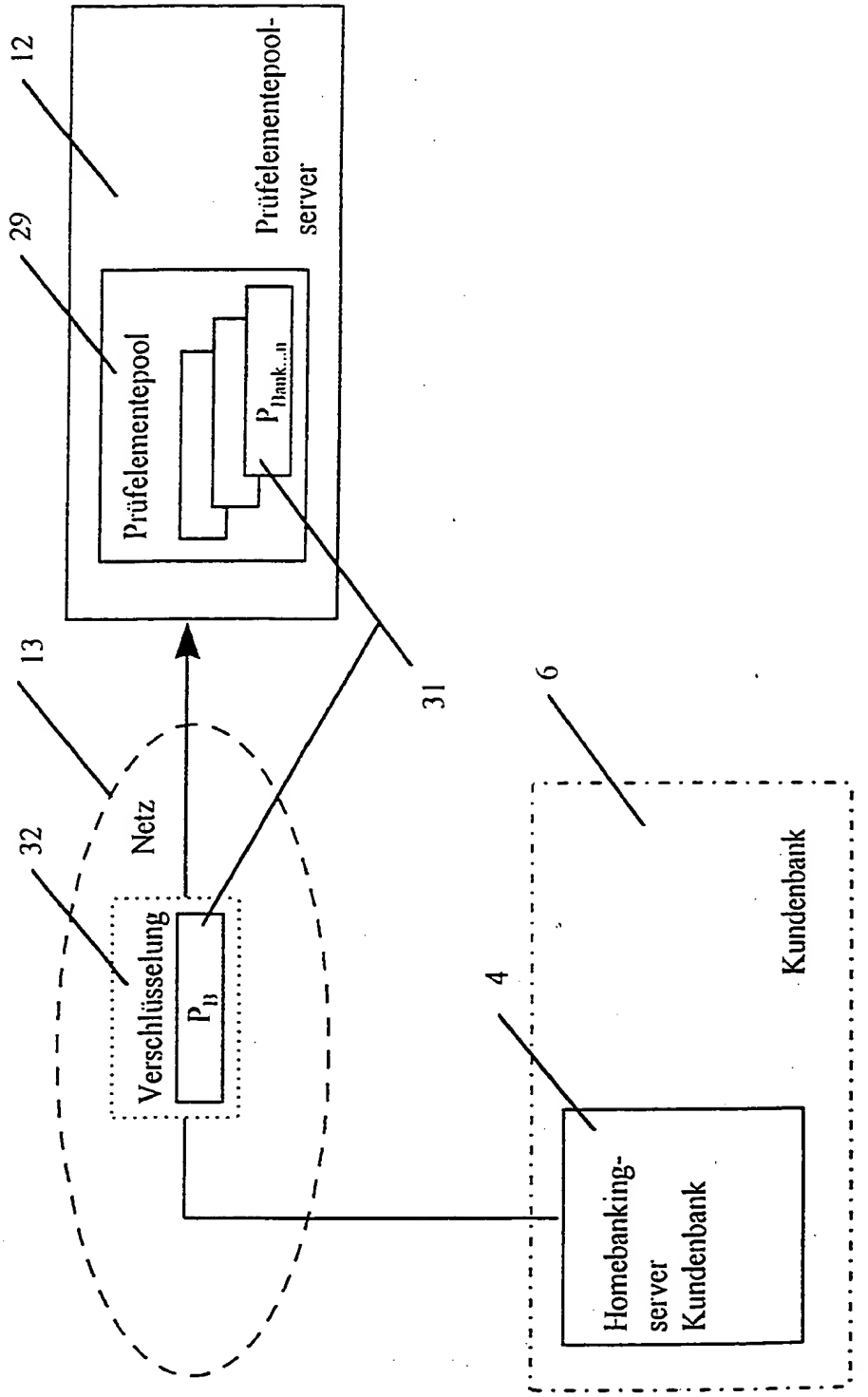
Figur 4

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



Figur 5

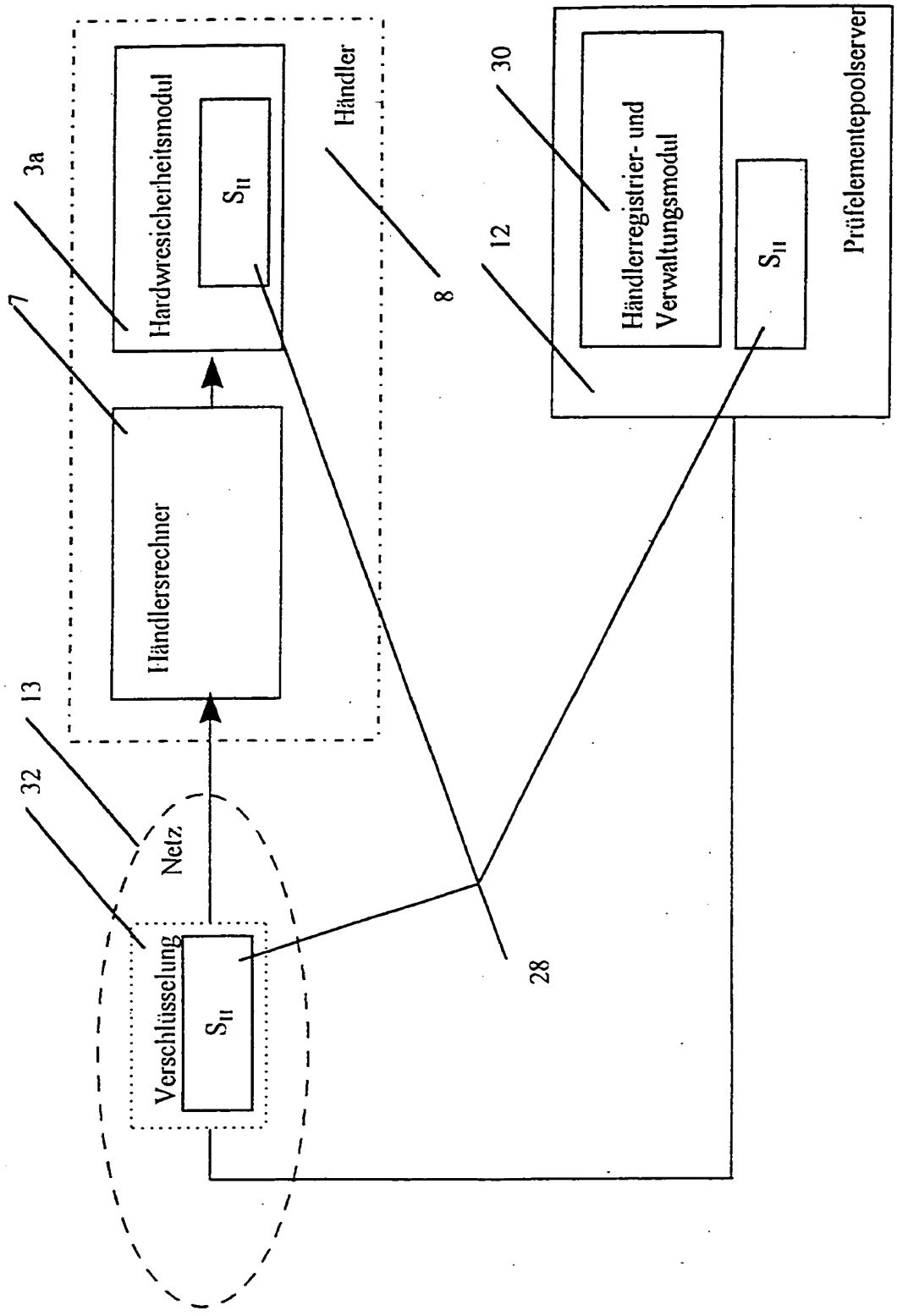
Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



Figur 6

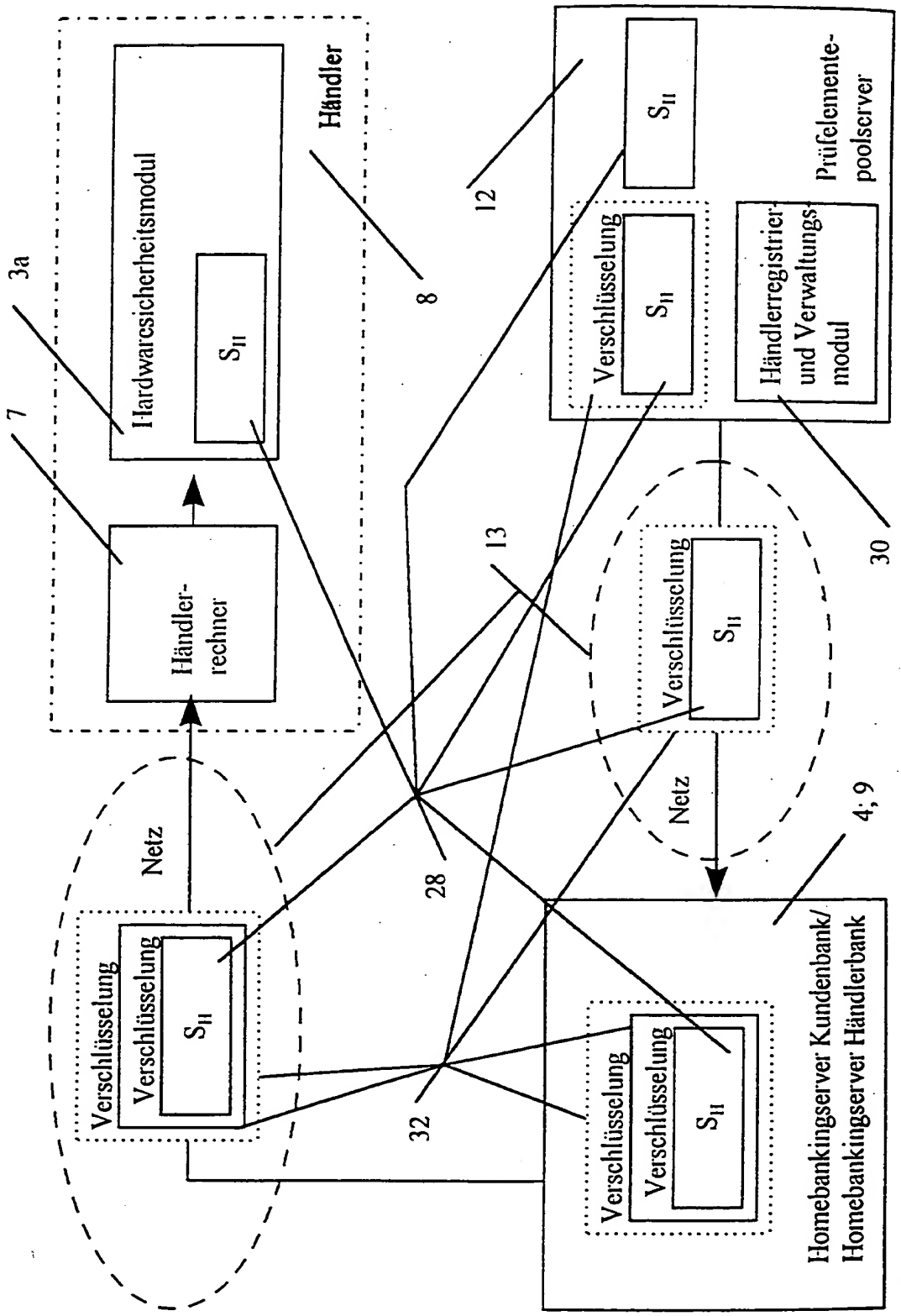
Schritt 1

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



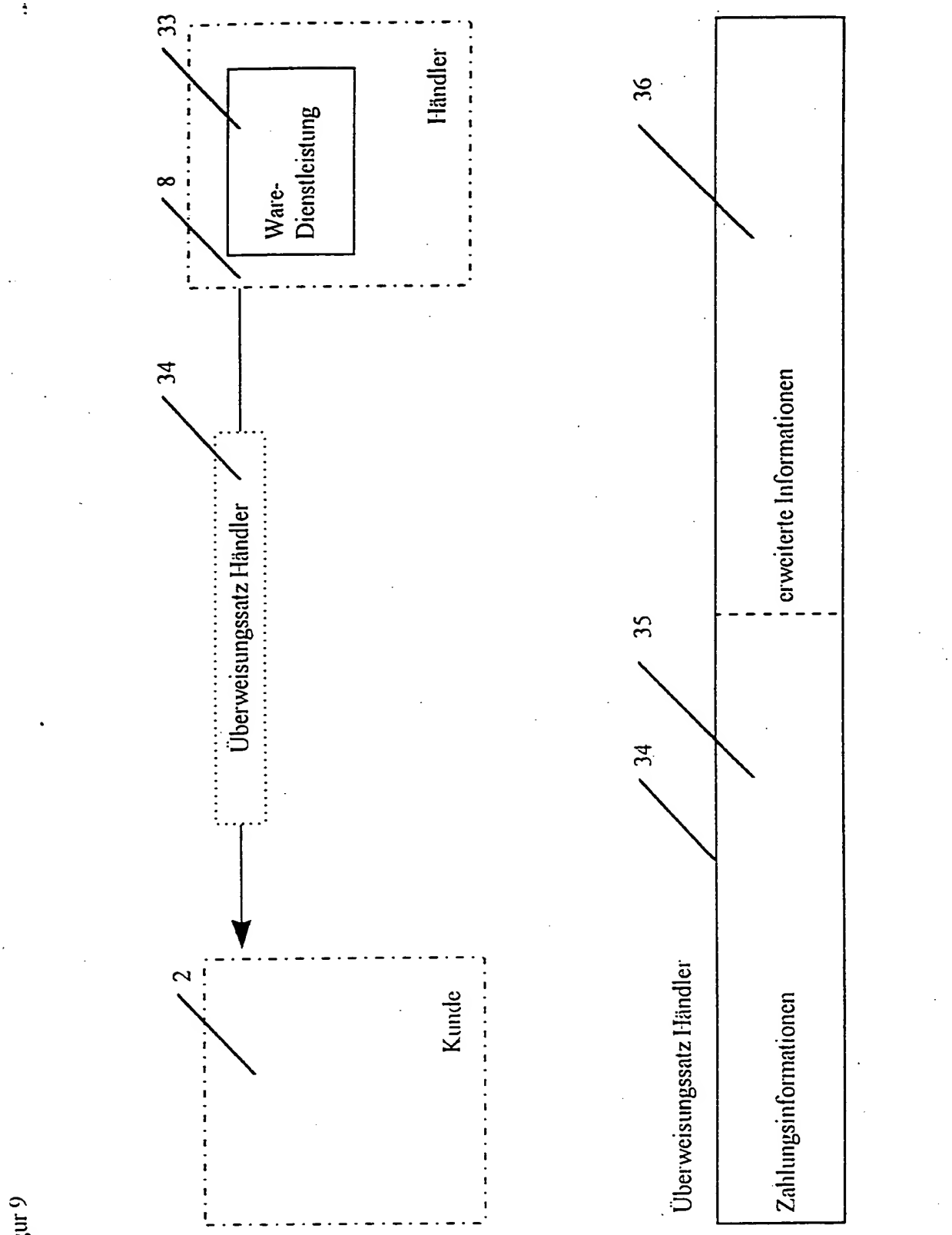
Figur 7

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



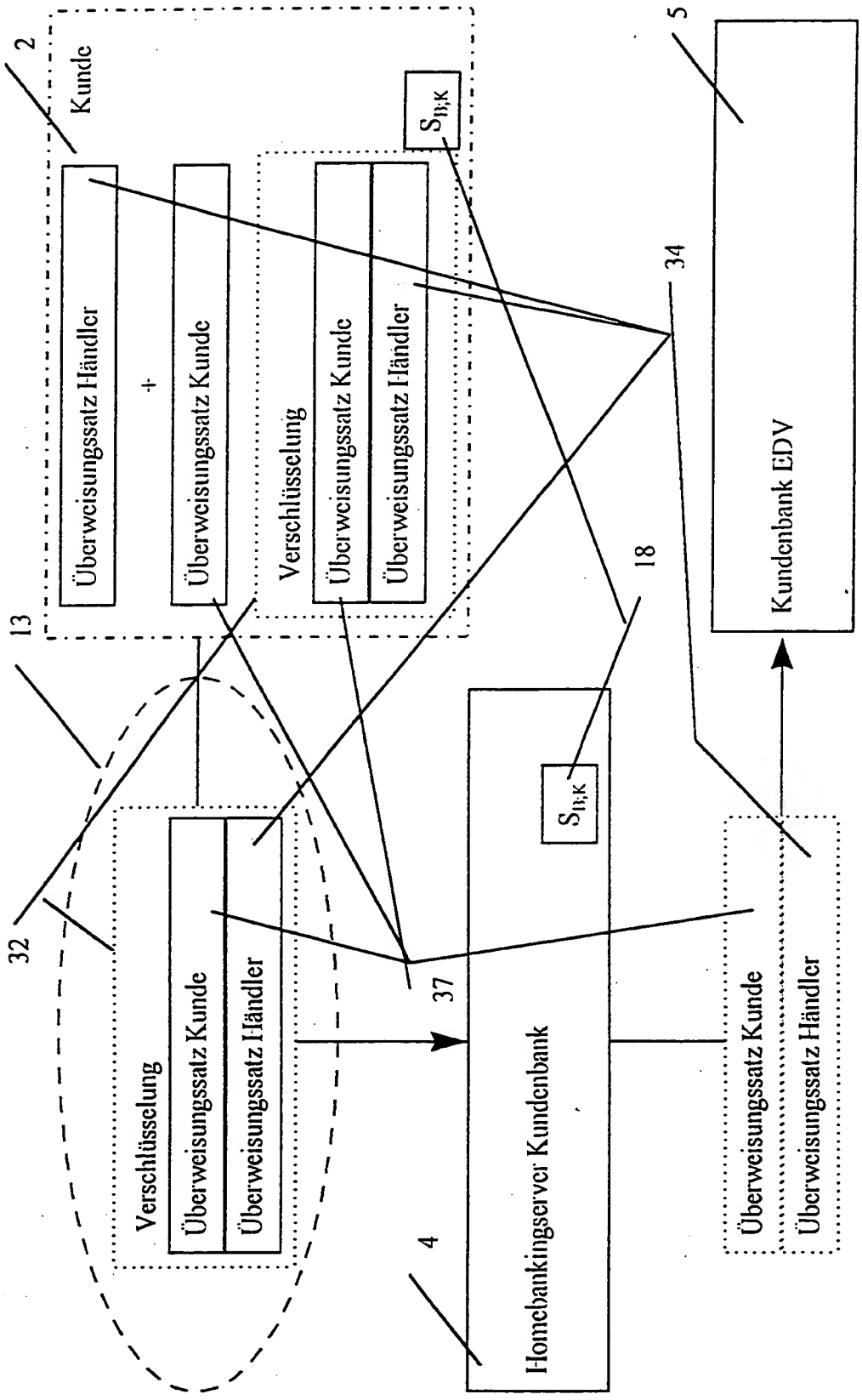
Figur 8

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



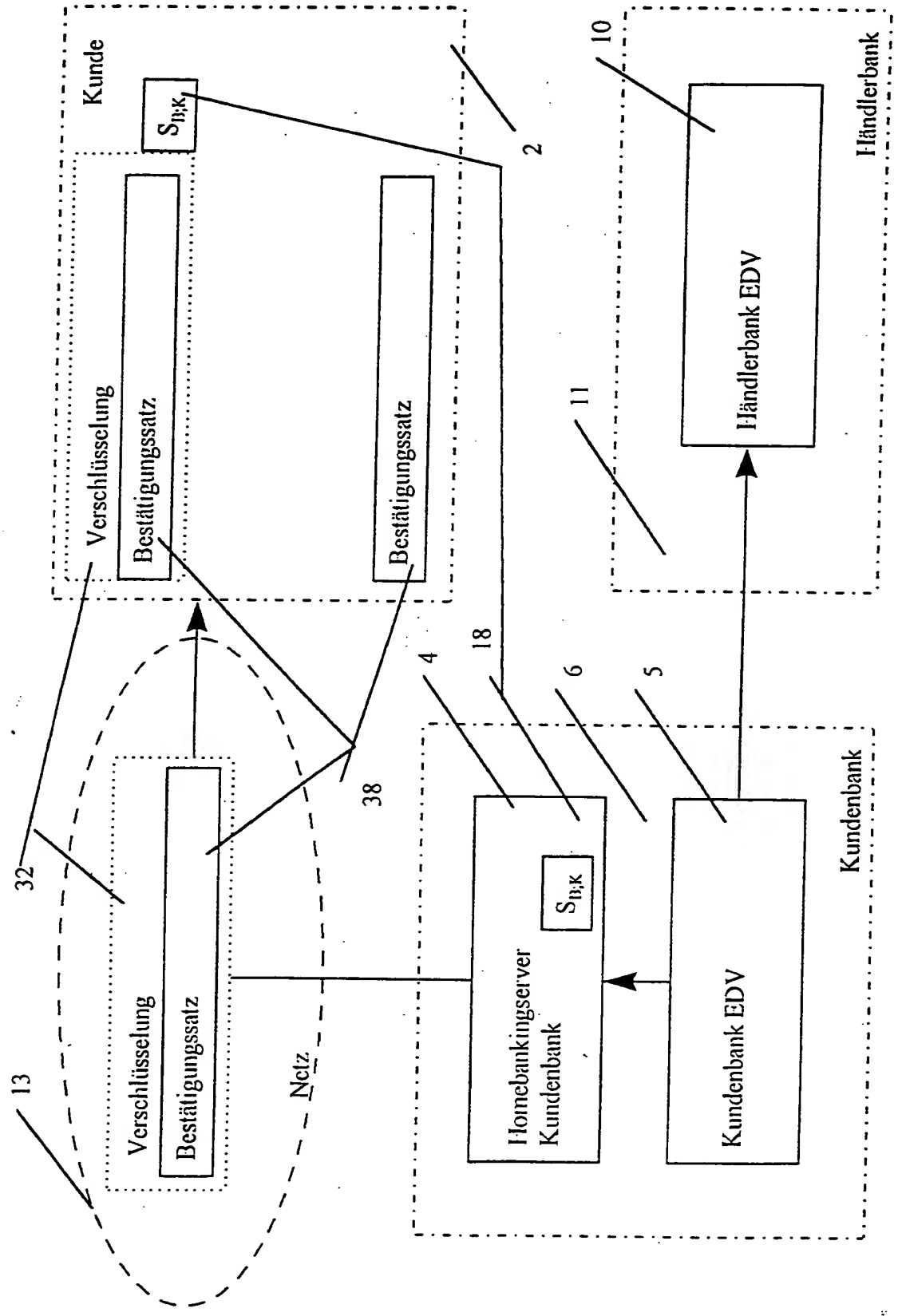
Figur 9

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



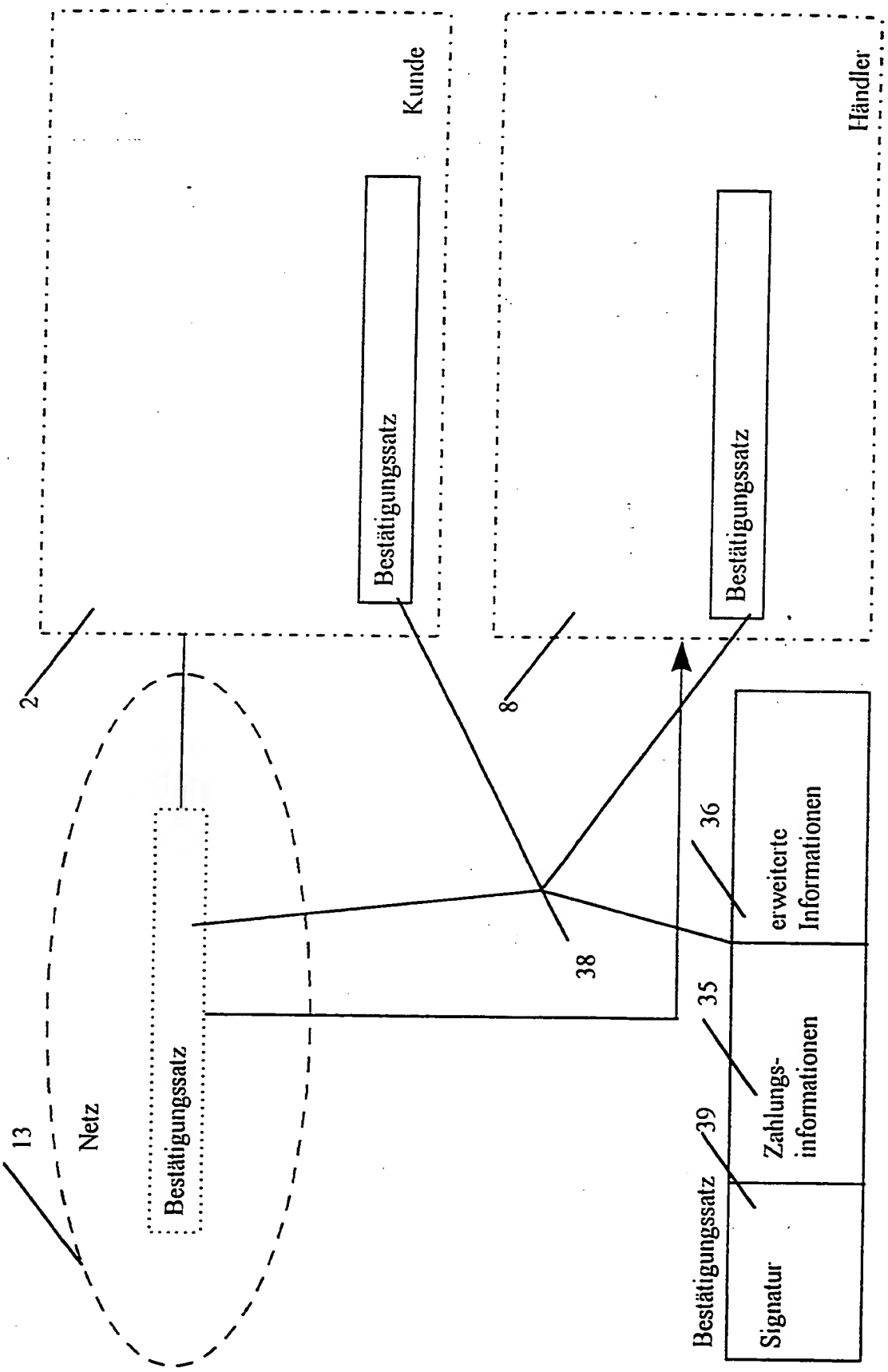
Figur 10

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenl gungstag: 22. Januar 1998



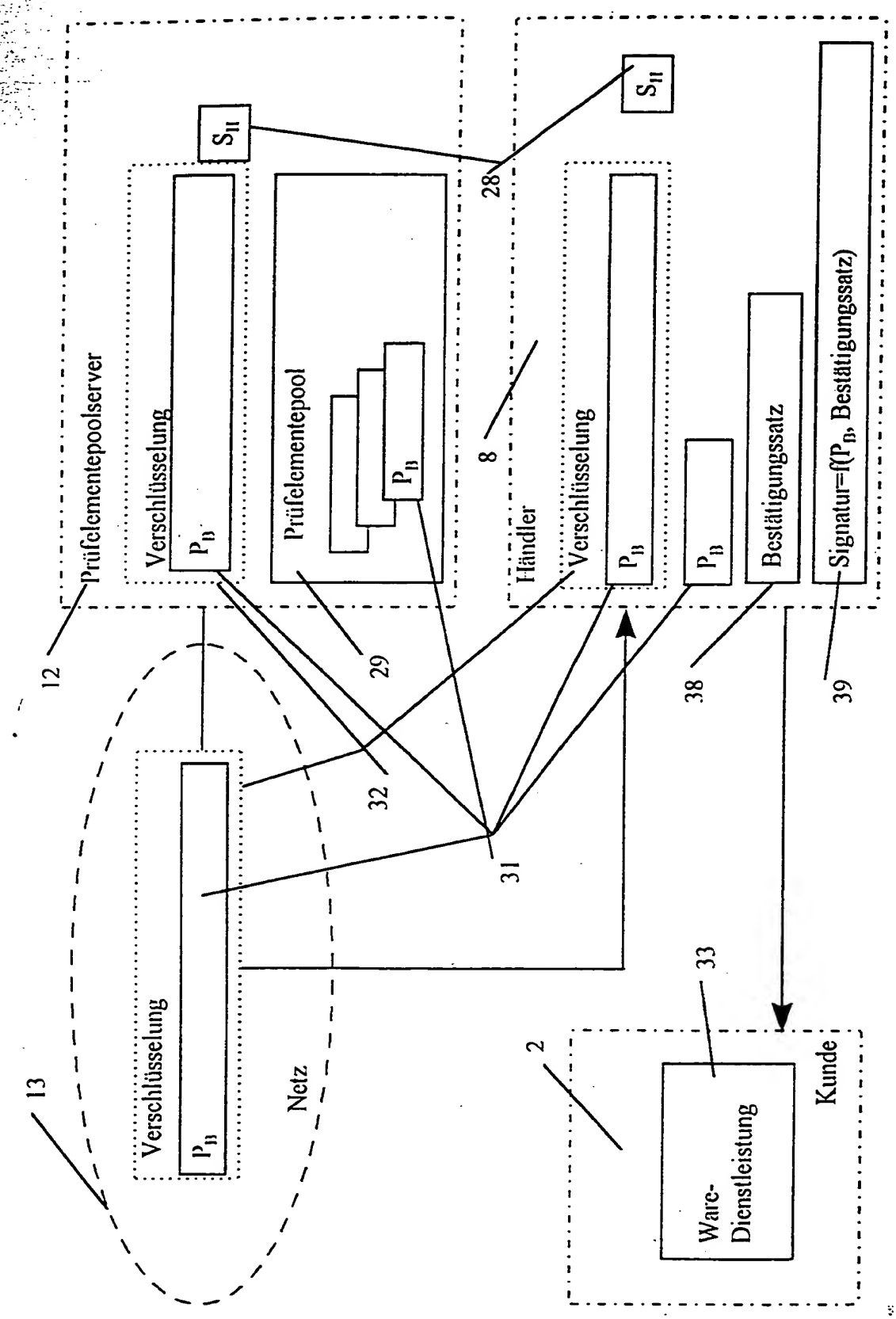
Figur 11

Nummer: DE 196 28 049 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



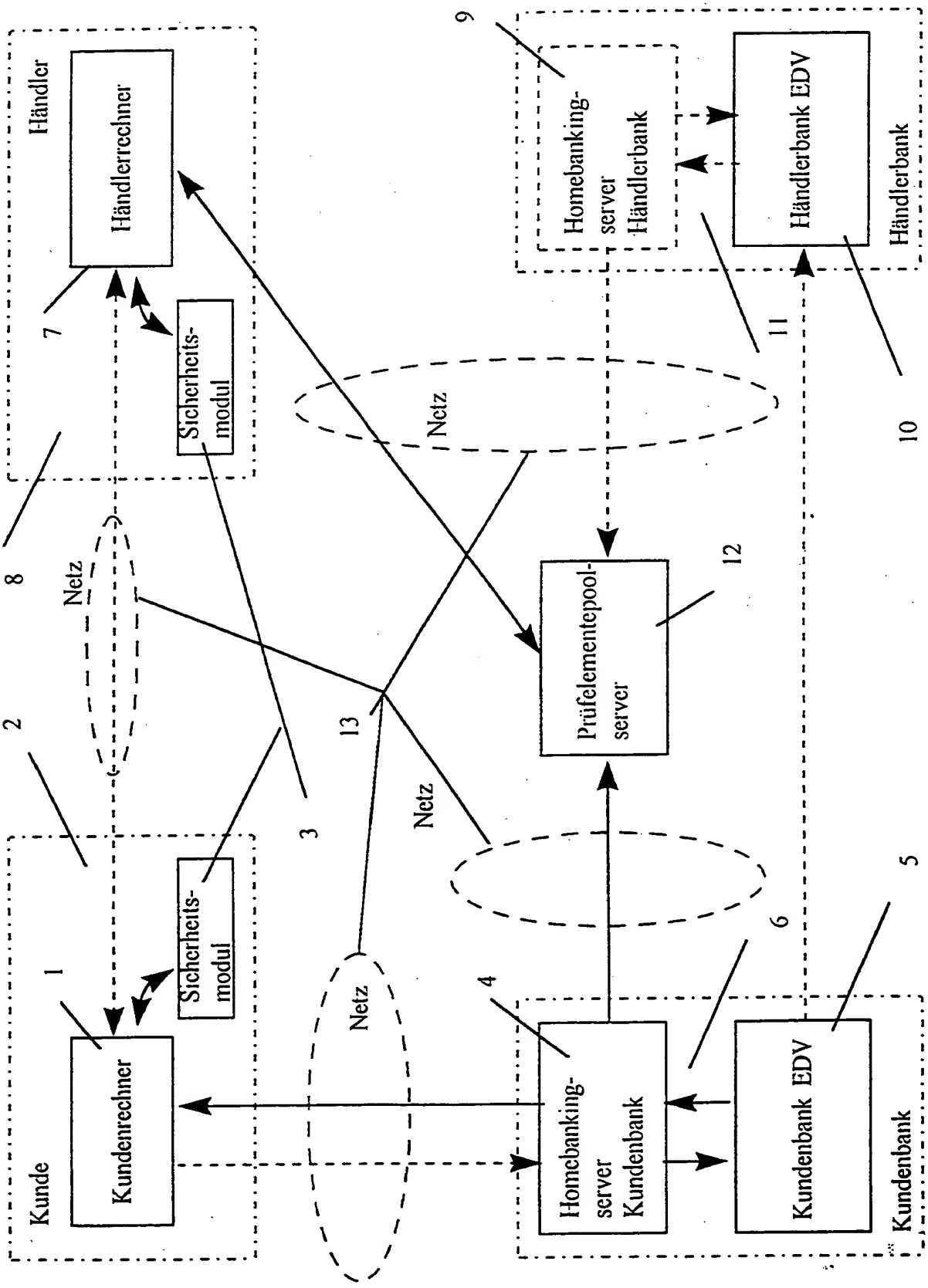
Figur 12

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



Figur 13

Nummer: DE 196 28 045 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 22. Januar 1998



Figur 1